CLAIMS:

1. A method of generating an Authorized Domain (AD), the method comprising the steps of

- selecting a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (100),
- binding at least one user (P1, P2, ..., PN_1) to the domain identifier (Domain_ID), and
- binding at least one device (D1, D2, ..., DM) to at least one user (P1, P2, ..., PN_1),
- thereby obtaining a number of devices (D1, D2, ..., DM) and a number of users (P1, P2, ..., PN_1) that is authorized to access a content item (C1, C2, ..., CN_2) of said Authorized Domain (100).

2. A method according to claim 1, characterized in that

- each device (D1, D2, ..., DM) may be bound to only a single user, or
- each device (D1, D2, ..., DM) may be bound to several users, where one user is indicated as a primary user for that particular device (D1, D2, ..., DM).

3. A method according to claim 2, characterized in that the method further comprises the step of:

- importing, on a given device (D1, D2, ..., DM), at least one content item (C1, C2, ..., CN_2) into the Authorized Domain (AD) given by the domain identifier (Domain_ID) by
- automatically binding, by default, the at least one imported content item (C1, C2, ..., CN_2) to the single user (P1, P2, ..., PN_1) that the given device (D1, D2, ..., DM) is bound to or to the user (P1, P2, ..., PN_1) indicated as primary user for the given device (D1, D2, ..., DM), or
- binding the at least one imported content item (C1, C2, ..., CN_2) to another user (P1, P2, ..., PN_1) using additional information, when non-default binding is to be used.

4. A method according to any of claims 1 – 3, characterized in that the method further comprises

- providing an Authorized Domain (AD) size limitation, where the limitation relates to a maximum number of users.

5. A method according to any of claims 1 – 4, characterized in that the method further comprises
using a user identification device as a personal Authorized Domain (AD) manager, and/or
using a personal mobile device as a personal Authorized Domain manager, and/or
using a mobile phone as a personal Authorized Domain manager, and/or
using a PDA (personal digital assistant) as a personal Authorized Domain manager and/or.

6. A method according to any of claims 1 – 5, characterized in that the step of binding at least one user (P1, P2, ..., PN_1) to the domain identifier (Domain_ID) comprises:
obtaining or generating a Domain Users List (DUC) comprising the domain identifier (Domain_ID) and a unique identifier (Pers_ID1, Pers_ID2, ..., $Pers\_IDN_1$) for a user (P1, P2, ..., PN_1) thereby defining that the user is bound to the Authorized Domain (100).

7. A method according to any of claims 1 – 6, characterized in that
the step of binding at least one device (D1, D2, ..., DM) to at least one user (P1, P2, ..., PN_1) comprises
obtaining or generating a Device Owner List (DOC) comprising a unique identifier (Pers_ID1, Pers_ID2, ..., $Pers\_IDN_1$) for a user (P1, P2, ..., PN_1) and a unique identifier (Dev_ID1, Dev_ID2, ..., Dev_IDM) for each device (D1, D2, ..., DM) belonging to the user thereby defining that the at least one device is/are bound to the user (P1, P2, ..., PN_1),
or in that the step of binding at least one device (D1, D2, ..., DM) to at least one user (P1, P2, ..., PN_1) comprises
obtaining or generating a Device Owner List (DOC) for each device (D1, D2, ..., DM) to be bound, the Device Owner List (DOC) comprising a unique identifier (Pers_ID1, Pers_ID2, ..., $Pers\_IDN_1$) for a user (P1, P2, ..., PN_1) and a unique identifier (Dev_ID1, Dev_ID2, ..., Dev_IDM) for a device (D1, D2, ..., DM) belonging to the user thereby defining that the device is bound to the user (P1, P2, ..., PN_1).

8. A method according to any of claims 1 – 7, characterized in that the step of binding at least one content item (C1, C2, ..., CN_2) to the Authorized Domain (AD) comprises:

binding a content item (C1, C2, ..., CN_2) to a User Right (URC1, URC2, ... $URCN_2$), where said User Right (URC1, URC2, ... $URCN_2$) is bound to a user (P1, P2, ..., PN_1) bound to the Authorized Domain (100).

9. A method according to claim 8, characterized in that the User Right (URC1, URC2, ... $URCN_2$) comprises rights data (Rghts Dat) representing which rights exists in relation to the at least one content item (C1, C2, ..., CN_2) bound to the User Right (URC1, URC2, ... $URCN_2$).

10. A method according to any one of the previous claims, characterized in that the method further comprises the step of controlling access, by a given device being operated by a given user, to a given content item (C1, C2, ..., CN_2), the step comprising:
checking whether a user, the given content item (C1, C2, ..., CN_2) is linked to, and a user, the given device is linked to, belongs to the same Authorized Domain (AD), and allowing access for the given user and/or other users via the given device to the content item if so,
and/or
checking if the given content item (C1, C2, ..., CN_2) is linked to a user belonging to the same Authorized Domain (AD) as the given user, and allowing access for the given user via the given device and/or other devices to the content item if so.

11. A method according to any one of claims 6 – 9, characterized in that the method further comprises the step of controlling access, by a given device being operated by a given user, to a given content item (C1, C2, ..., CN_2) being bound to the Authorized Domain (100) and having a unique content identifier (Cont_ID), comprising:
checking if the Domain User List (DUC) of the Authorized Domain (100) comprises both a first user identifier (Pers_ID), comprised in a Device Owner List (DOC) comprising an identifier (Dev1_ID, Dev2_ID) of the given device, and a second user identifier (Pers_ID), linked to the given content item (C1, C2, ..., CN_2), thereby checking if the user bound to the given device is bound to the same Authorized Domain (100) as the user bound to the content item, and
allowing access to the given content item (C1, C2, ..., CN_2) by the given device (D1, D2, ..., DM) operated by any user
and/or
checking if the Domain User List (DUC) of the Authorized Domain (100), that the content

item is bound to, comprises a user identifier (Pers_ID) of the given user (P1, P2, ..., PN_1) thereby checking if the given user is bound to the same Authorized Domain (100) as the content item, and

allowing access to the given content item (C1, C2, ..., CN_2) by any device including the given device operated by the given user.

12. A method according to any of claims 10 – 11, characterized in that the step of controlling access of a given content item further comprises:

checking that the User Right (URC1, URC2, ... $URCN_2$) for the given content item specifies that the given user (P1, P2, ..., PN_1) has the right to access the given content item (C1, C2, ..., CN_2) and only allowing access to the given content item (C1, C2, ..., CN_2) in the affirmative.

13. A method according to any of claims 1 – 12, characterized in that every content item is encrypted and that a content right (CR) is bound to each content item and to a User Right (URC1, URC2, ... $URCN_2$), and that the content right (CR) of a given content item comprises a decryption key for decrypting the given content item.

14. A method according to any of claims 6 – 13, characterized in that

the Domain Users List (DUC) is implemented as or included in a Domain Users Certificate, and/or

the Device Owner List (DOC) is implemented as or included in a Device Owner Certificate, and/or

the User Right (URC1, URC2, ..., $URCN_2$) is implemented as or included in a User Right Certificate.

15. A method according to any previous claim, characterized by binding at least one content item (C1, C2, ..., CN_2) to at least one user (P1, P2, ..., PN_1).

16. A system for generating an Authorized Domain (AD), the system comprising:

means for obtaining a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (100),

means for binding at least one user (P1, P2, ..., PN_1) to the domain identifier (Domain_ID), and

means for binding at least one device (D1, D2, ..., DM) to at least one user (P1, P2, ..., PN_1), thereby obtaining a number of devices (D1, D2, ..., DM) and a number of persons (P1, P2, ..., PN_1) that is authorized to access a content item of said Authorized Domain (100).

17. A system according to claim 16, characterized in that
each device (D1, D2, ..., DM) may be bound to only a single user, or
each device (D1, D2, ..., DM) may be bound to several users, where one user is indicated as a primary user for that particular device (D1, D2, ..., DM).

18. A system according to claim 17, characterized in that the system further comprises means for:
importing, on a given device (D1, D2, ..., DM), at least one content item (C1, C2, ..., CN_2) into the Authorized Domain (AD) given by the domain identifier (Domain_ID) by automatically binding, by default, the at least one imported content item (C1, C2, ..., CN_2) to the single user (P1, P2, ..., PN_1) that the given device (D1, D2, ..., DM) is bound to or to the user (P1, P2, ..., PN_1) indicated as primary user for the given device (D1, D2, ..., DM), or binding the at least one imported content item (C1, C2, ..., CN_2) to another user (P1, P2, ..., PN_1) using additional information, when non-default binding is to be used.

19. A system according to any of claims 16 – 18, characterized in that the system further comprises means for
providing an Authorized Domain (AD) size limitation, where the limitation relates to a maximum number of users.

20. A system according to any of claims 16 – 19, characterized in that the system further comprises means for:
using a user identification device as a personal Authorized Domain (AD) manager, and/or
using a personal mobile device as a personal Authorized Domain manager, and/or
using a mobile phone as a personal Authorized Domain manager, and/or
using a PDA (personal digital assistant) as a personal Authorized Domain manager.

21. A system according to any of claims 16 – 20, characterized in that the means for binding at least one user (P1, P2, ..., PN_1) to the domain identifier (Domain_ID) is adapted to:

obtain or generate a Domain Users List (DUC) comprising the domain identifier (Domain_ID) and a unique identifier (Pers_ID1, Pers_ID2, ..., Pers_IDN$_1$) for a user (P1, P2, ..., PN$_1$) thereby defining that the user is bound to the Authorized Domain (100).

22. A system according to any of claims 16 – 21, characterized in that the means for binding at least one device (D1, D2, ..., DM) to at least one user (P1, P2, ..., PN$_1$) is adapted to
obtain or generate a Device Owner List (DOC) comprising a unique identifier (Pers_ID1, Pers_ID2, ..., Pers_IDN$_1$) for a user (P1, P2, ..., PN$_1$) and a unique identifier (Dev_ID1, Dev_ID2, ..., Dev_IDM) for each device (D1, D2, ..., DM) belonging to the user thereby defining that the at least one device is/are bound to the user (P1, P2, ..., PN$_1$),
or in that the means for binding at least one device (D1, D2, ..., DM) to at least one user (P1, P2, ..., PN$_1$) is adapted to
obtain or generate a Device Owner List (DOC) for each device (D1, D2, ..., DM) to be bound, the Device Owner List (DOC) comprising a unique identifier (Pers_ID1, Pers_ID2, ..., Pers_IDN$_1$) for a user (P1, P2, ..., PN$_1$) and a unique identifier (Dev_ID1, Dev_ID2, ..., Dev_IDM) for a device (D1, D2, ..., DM) belonging to the user thereby defining that the device is bound to the user (P1, P2, ..., PN$_1$).

23. A system according to any of claims 16 – 22, characterized in that the means for binding at least one content item (C1, C2, ..., CN$_2$) to the Authorized Domain (AD) is adapted to:
bind a content item (C1, C2, ..., CN$_2$) to a User Right (URC1, URC2, ... URCN$_2$), where said User Right (URC1, URC2, ... URCN$_2$) is bound to a user (P1, P2, ..., PN$_1$) bound to the Authorized Domain (100).

24. A system according to claim 23, characterized in that the User Right (URC1, URC2, ... URCN$_2$) comprises rights data (Rghts Dat) representing which rights exists in relation to the at least one content item (C1, C2, ..., CN$_2$) bound to the User Right (URC1, URC2, ... URCN$_2$).

25. A system according to any of claims 16 – 24, characterized in that the system further comprises the means for controlling access, by a given device being operated by a given user, to a given content item (C1, C2, ..., CN$_2$), where the means is adapted to:

check whether a user, the given content item (C1, C2, ..., CN_2) is linked to, and a user, the given device is linked to, belongs to the same Authorized Domain (AD), and allowing access for the given user and/or other users via the given device to the content item if so,
and/or
check if the given content item (C1, C2, ..., CN_2) is linked to a user belonging to the same Authorized Domain (AD) as the given user, and allowing access for the given user via the given device and/or other devices to the content item if so.

26. A system according to any one of claims 21 – 25, characterized in that the system further comprises means for controlling access, by a given device being operated by a given user, to a given content item (C1, C2, ..., CN_2) being bound to the Authorized Domain (100) and having a unique content identifier (Cont_ID), where the means is adapted to:
check if the Domain User List (DUC) of the Authorized Domain (100) comprises both a first user identifier (Pers_ID), comprised in a Device Owner List (DOC) comprising an identifier (Dev1_ID, Dev2_ID) of the given device, and a second user identifier (Pers_ID), linked to the given content item (C1, C2, ..., CN_2), thereby checking if the user bound to the given device is bound to the same Authorized Domain (100) as the user bound to the content item,
and
allow access to the given content item (C1, C2, ..., CN_2) by the given device (D1, D2, ..., DM) operated by any user
and/or
check if the Domain User List (DUC) of the Authorized Domain (100), that the content item is bound to, comprises a user identifier (Pers_ID) of the given user (P1, P2, ..., PN_1) thereby checking if the given user is bound to the same Authorized Domain (100) as the content item,
and
allow access to the given content item (C1, C2, ..., CN_2) by any device including the given device operated by the given user.

27. A system according to any of claims 25 – 26, characterized in that the means for controlling access of a given content item is further adapted to:
check that the User Right (URC1, URC2, ... $URCN_2$) for the given content item specifies that the given user (P1, P2, ..., PN_1) has the right to access the given content item (C1, C2, ..., CN_2) and only allow access to the given content item (C1, C2, ..., CN_2) in the affirmative.

28. A system according to any of claims 16 – 27, characterized in that every content item is encrypted and that a content right (CR) is bound to each content item and to a User Right (URC1, URC2, ... $URCN_2$), and that the content right (CR) of a given content item comprises a decryption key for decrypting the given content item.

29. A system according to any of claims 20 – 28, characterized in that
the Domain Users List (DUC) is implemented as or included in a Domain Users Certificate, and/or
the Device Owner List (DOC) is implemented as or included in a Device Owner Certificate, and/or
the User Right (URC1, URC2, ..., $URCN_2$) is implemented as or included in a User Right Certificate.

30. A computer readable medium having stored thereon instructions for causing one or more processing units to execute the method according to any one of claims 1 – 15.

31. An Authorized Domain (AD) characterized in that the Authorized Domain (AD) has been generated by the method according to any one of claims 1 – 15 or by the system according to any one of claims 16 – 29.

32. An Authorized Domain (AD) structure comprising
a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (100),
a representation of at least one user (P1, P2, ..., PN_1) bound to the domain identifier (Domain_ID), and
a representation of at least one device (D1, D2, ..., DM) bound to at least one user (P1, P2, ..., PN_1),
thereby defining a number of devices (D1, D2, ..., DM) and a number of users (P1, P2, ..., PN_1) that is authorized to access a content item (C1, C2, ..., CN_2) of said Authorized Domain (100).